УДК 621.311

ОЦЕНКА ВЛИЯНИЯ РАЗМЕРА ЗАПАСОВ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Е.П. Соколовский
Краснодарское высшее военное училище (военный институт)
Россия, 350063, Краснодар, Красина ул., 4
E-mail: biryza_08@mail.ru

О.А. Финько
Краснодарское высшее военное училище (военный институт)
Россия, 350063, Краснодар, Красина ул., 4
E-mail: ofinko@yandex.ru

Ключевые слова: информационная безопасность, система защиты информации, расчет запасов, логико-вероятностный метод.

Воздействие угроз информационной безопасности на объект информатизации и систему защиты информации порождает слабо прогнозируемый спрос на израсходованные (утраченные) элементы средств защиты информации. Для обеспечения функционирования системы защиты с требуемым качеством необходимо иметь некоторый запас наиболее востребованных элементов. Создание чрезмерных запасов элементов связано с возрастанием издержек хранения, которые, предположительно, будут негативно влиять на обеспечение информационной безопасности организации. На основе известных положений управления рисками информационной безопасности, шкалирования и логико-вероятностного метода И.А. Рябинина предложены элементы методики оценки влияния размера запаса элементов на обеспечение информационной безопасности организации.

EVALUATION OF THE INFLUENCE THE SIZE OF INVENTORIES OF TOOLS OF INFORMATION PROTECTION ON ASSURING INFORMATION SAFETY OF THE ORGANIZATION

E.P. Sokolovsky
Krasnodar Higher Military College (military institute)
Russia, 350063, Krasnodar, Krasina Street, 4
E-mail: biryza_08@mail.ru

O.A. Finko
Krasnodar Higher Military College (military institute)
Russia, 350063, Krasnodar, Krasina Street, 4
E-mail: ofinko@yandex.ru

Key words: information safety, system of information protection, inventory calculation, logic and probabilistic method.

Exposure of threats of information safety to an object of informatization and system of information protection generates a weakly predicted demand on expended (lost) elements of tools of information protection. To provide performance of protection systems with a required quality, one should have some inventory of mostly demanded elements. Creating excessive inventory of elements is concerned with increasing costs that, supposedly, will negatively influence assuring information safety of the organization. On the basis of known guidelines of control of risks of the information safety, scaling, logic-probabilistic method of I.A. Ryabinin, elements of a procedure of evaluation of the size of inventory of elements on assuring the information safety of the organization are proposed.

1. Введение

Под *объектом информатизации* понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств) в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [1]. Объект информатизации, а также создаваемая для обеспечения его информационной безопасности (ИБ)[1] система защиты информации (ЗИ)[2], подвержены воздействию угроз ИБ [3, 4]. При этом под *угрозой* ИБ понимается совокупность факторов и условий, создающих опасность нарушения ИБ организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации [2].

Как известно, защищенность достигается обеспечением совокупности свойств ИБ – конфиденциальности, целостности и доступности информационных активов. Приоритетность свойств ИБ определяется значимостью информационных активов для интересов (целей) организации. Непосредственное обеспечение ИБ достигается за счет использования средств защиты информации (СрЗИ)[3].

Функционирование системы ЗИ подразумевает расходование *элементов* СрЗИ, которое может быть:

- постепенным (прогнозируемым) — например, в результате реализации угроз физического износа или выхода из строя элементов СрЗИ;
- внезапным (случайным) — например, в результате реализации угроз воздействия нарушителя или аварии (пожара).

Рассматриваются такие системы ЗИ, для которых создается *запас наиболее востребованных элементов СрЗИ* с целью обеспечения требуемого качества[4] функционирования. Например, для обеспечения свойств конфиденциальности информации используются *симметричные криптографические системы,* под которыми понимается семейство T обратимых преобразований открытого текста в шифрованный. Членам этого семейства можно взаимно однозначно сопоставить число k, называемое *ключом*[5] [6]. Оп-

[1] Информационная безопасность (ИБ) – состояние защищенности интересов организации в условиях угроз в информационной сфере [2].

[2] Система ЗИ – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации [3].

[3] СрЗИ – техническое, программное, программно-техническое средство (вещество) и (или) материал, предназначенные или используемые для защиты информации [3].

[4] Качество – совокупность характеристик объекта, имеющая отношение к его способности удовлетворить установленные и предполагаемые требования потребителя [5].

[5] Ключ – конкретное конфиденциальное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма [6].

ределение размера запасов ключей для симметричных криптографических систем целесообразно осуществлять с использованием *экспертных систем*, предназначенных для решения качественных задач с помощью накапливаемых знаний и получения логических выводов [7, 8].

При управлении запасами ключей очевидны следующие варианты реализации угроз и рисков ИБ для объекта информатизации и системы ЗИ.

1) Невозможность своевременного восстановления израсходованного (выведенного из строя) ключа оказывает негативное влияние на качество функционирования криптографической системы и является угрозой ИБ.
2) Излишний запас ключей вызывает риски ИБ[6], связанные с издержками хранения:

- нарушением в процессе хранения свойств целостности, доступности и конфиденциальности ключей;
- потерей качества ключей в результате устаревания, естественного разрушения в процессе хранения или возникновения стихийных бедствий (пожара и пр.)

Очевидно, что необходимо оценивать влияние размера запаса элементов СрЗИ на обеспечение ИБ, особенно в распределенных крупномасштабных системах управления (например, в структуре министерств, ведомств, корпоративных систем управления).

2. Оценка влияния запаса элементов СрЗИ на ИБ организации

2.1. Постановка задачи

Рассматривается промежуток времени в один период T. На объект случайным образом поступают заявки на обеспечение элементами СрЗИ. Для выполнения заявки в случайный момент времени необходим некоторый запас элементов. Задача заключается в оценке влияния размера запаса на риски ИБ, связанные с издержками хранения.

2.2. Расчет запаса элементов СрЗИ без издержек хранения

Пусть R – количество элементов СрЗИ в конце периода. В условиях задачи справедливым будет равенство:

$$R = r - \sum_{j=1}^{N} Y_j ,$$

где r – запас элементов СрЗИ на начало периода, N – число поступивших заявок на обеспечение элементами, Y_j – количество элементов, необходимое для выполнения j-ой заявки.

В рамках модели допустим, что N – пуассоновская случайная величина с интенсивностью λ, Y_j – независимые одинаково распределенные случайные величины с математическим ожиданием $M[Y_j] = \alpha$ и дисперсией $D[Y_j] = \beta^2$; N; $Y_1, ..., Y_j$; N и Y_j – независимы.

Для обеспечения непрерывности выполнения заявок необходимо, чтобы количество элементов СрЗИ на конец периода T оказалось неотрицательным с вероятностью не менее заданной величины:

[6] Риск ИБ – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [9].

$$P(R \geq 0) = Q,$$

где Q – значение вероятности того, что запас R будет неотрицательным.

Согласно [10, 11] функция вероятности обеспечения потребности в элементах СрЗИ в зависимости от r представляется выражением:

$$Q(r) = \Phi\left(\frac{r-\lambda\alpha}{\sqrt{\lambda(\alpha^2+\beta^2)}}\right), \quad (1)$$

для определения величины r используется формула:

$$r = \lambda\alpha + \Phi^{-1}(Q)\sqrt{\lambda(\alpha^2+\beta^2)}, \quad (2)$$

где $\Phi^{-1}(Q)$ – квантиль уровня Q стандартной нормальной случайной величины.

Например, на объект за период времени T в среднем поступает $\lambda = 70$ заявок на обеспечение элементами СрЗИ. Для выполнения заявки в среднем используется $\alpha = 2$ элемента, $\beta = 1$ – стандартное нормальное отклонение количества элементов, необходимых для выполнения одной заявки. Требуемая вероятность обеспечения потребности в элементах $Q(r) = 0,95$. В соответствии с (2) для данных условий нам необходимо $r = 170,7724 \approx 171$, что является размером запаса без издержек хранения.

2.3. Элементы методики оценки влияния запаса элементов СрЗИ на обеспечение ИБ организации

Для определения влияния размера запаса на ИБ организации нужна произвольная функция издержек от размера запасов, обладающая следующими свойствами:

- принимать значение нуль при количестве запасов равном нулю;
- возрастать;
- быть нормированной на единицу, т.е. при $r \to +\infty$ стремиться к единице;
- определенной только для неотрицательных значений аргумента;
- отражать издержки от накопления излишествующего количества элементов.

Согласно [12] указанными свойствами обладает *функция распределения* неотрицательной случайной величины. Известно [13], что самым неопределенным на полупрямой является *экспоненциальное* распределение, поэтому, не ограничивая общности, будем считать, что функция, описывающая зависимость издержек от выбранного размера запаса, будет иметь следующий вид:

$$F(r) = 1 - e^{-kr}, \quad (3)$$

где r – размер запаса элементов, который необходимо иметь на начало периода T, k – коэффициент влияния r на риски ИБ, связанные с хранением запасов элементов.

Очевидно, что чем большее значение принимает r, тем больше возрастают издержки хранения, определяемые (3). Обеспечение элементами СрЗИ осуществляется, как правило, в рамках *сложной системы*[7] обеспечения. В работах [15-17] приведено обоснование того, что в сложных системах сценарий реализации угроз (аварий) имеет логико-вероятностную природу. Поэтому инициирующие условия (угрозы ИБ) и их последствия (риски ИБ) могут быть связаны *логическими* связями, а математической основой для определения вероятности наступления негативного события является *логико-вероятностное исчисление*. Логико-вероятностный метод И.А. Рябинина (ЛВМ) позволяет не только оценить вероятность наступления риска ИБ (группы рисков ИБ), но и определить вклад каждого инициирующего условия (угрозы ИБ) в безопасное функ-

[7] Существуют различные определения понятия «сложная система». В рамках статьи под *сложной системой* понимается такая система, в модели которой не хватает информации для управления [14]

ционирование системы. Таким образом, коэффициент k может быть оценен как *вероятность* срыва в обеспечении элементами СрЗИ в результате нарушения свойств целостности, доступности, конфиденциальности элементов.

В общем виде ЛВМ оценки безопасности заключается в следующем [17].

Шаг 1. Экспертным путем строится сценарий перехода некоторой системы в опасное состояние, описываемый монотонной булевой функцией.

В соответствии с [17] построение сценария – творческий процесс, который должны осуществлять эксперты с учетом особенностей функционирования системы. Ясно, что значение параметра k зависит от ряда инициирующих условий: количества и квалификации персонала, приспособленности помещений для хранения запасов, организации и условий деятельности и т.д. Предполагаемый сценарий перехода системы обеспечения элементами СрЗИ к функционированию в опасном состоянии представлен на рис. 1.

Согласно [17] булеву функцию, связывающую состояние элементов с состоянием системы, будем называть *функцией опасного состояния системы* (ФОС). Под *вероятностной функцией* (ВФ) будем понимать вероятность истинности булевой функции

$$P\{f(\vec{\mathbf{z}})=1\},$$

где здесь и далее $f(\vec{\mathbf{z}})=[z_1 \quad \dots \quad z_n],\ z_1,\dots,\ z_n \in \{0,1\}$.

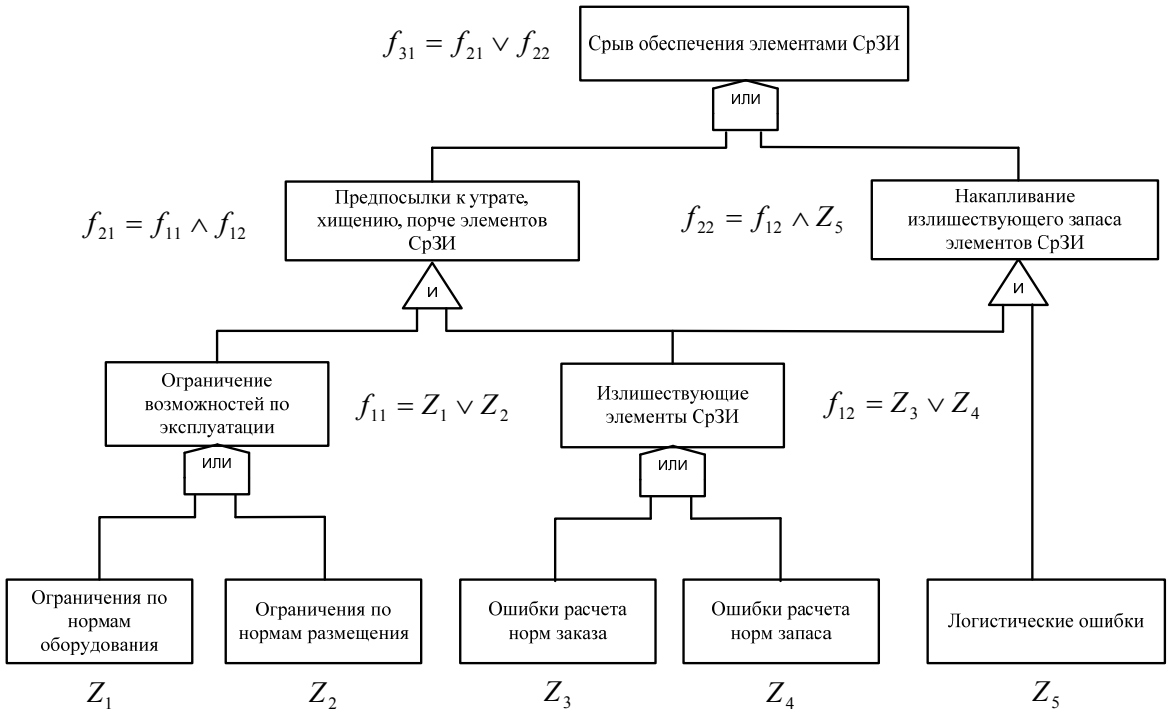

Рис. 1. Предполагаемый сценарий перехода системы обеспечения в опасное состояние.

Шаг 2. По правилам перехода из ФОС осуществляется получение арифметического полинома ВФ опасного состояния.

ФОС предполагаемого сценария (рис. 1) представим в бесповторной форме [17]:

$$y(Z_1,\dots,Z_5) = (Z_1 \vee Z_2)(Z_3 \vee Z_4) \vee (Z_3 \vee Z_4)Z_5 =$$
$$= (Z_3 \vee Z_4)((Z_1 \vee Z_2) \vee Z_5).$$

Для оценки k по правилам перехода [17] получим арифметический полином ВФ:

$$k = P\{(Z_1,\dots,Z_5)=1\} = [1-(1-Q_3)(1-Q_4)][1-((1-(1-(1-Q_1)(1-Q_2)))(1-Q_5)], \quad (4)$$

где Q_i – вероятность реализации Z_i угрозы ИБ в сценарии (рис. 1).

Шаг 3. На основании полученного арифметического полинома ВФ опасного состояния выполняется оценка безопасности системы.

Следует выбирать такие значения r и так планировать вопросы обеспечения элементами СрЗИ, чтобы издержки, определяемые (3), стремились к нулю. Для этого значение функции

(5) $$\Psi(r) = e^{-kr},$$

должно быть как можно больше (рис. 2).

Для оценки влияния r в сценарии (рис. 1) допустим:

- при $r = 171$ (без издержек хранения) вероятность реализации угрозы Z_4 будет минимальной ($Q_4 = 0,01$);
- $Q_1 = Q_2 = Q_3 = Q_5 = 0,01$.

Тогда в соответствии с (4) для $r = 171$ оценим $k = 0,001$. Из графической зависимости (рис. 2) видно, что с увеличением r функция (1) увеличивается. Вместе с тем возрастает и функция (3).

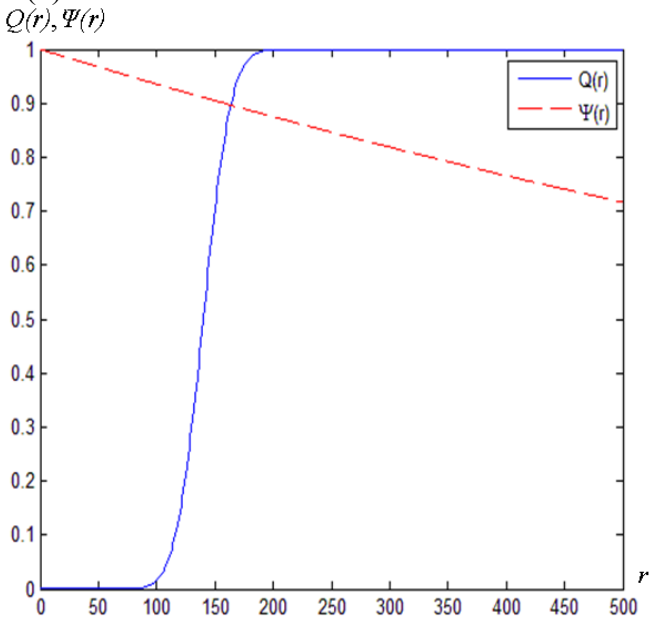

Рис. 2. Совместное представление графических зависимостей (1) и (5).

Для определения *оптимального* размера запаса элементов СрЗИ, очевидно, следует максимизировать функцию

(6) $$\Omega(r) = \frac{\Psi(r) + Q(r)}{2}.$$

Деление выполнено с целью нормировки для получения значений $0 \le \Omega(r) \le 1$.

Из графической зависимости (рис. 3) видно, что с учетом издержек, возникающих при хранении запасов, наибольшая вероятность обеспечения достигается при $r_R = 190$.

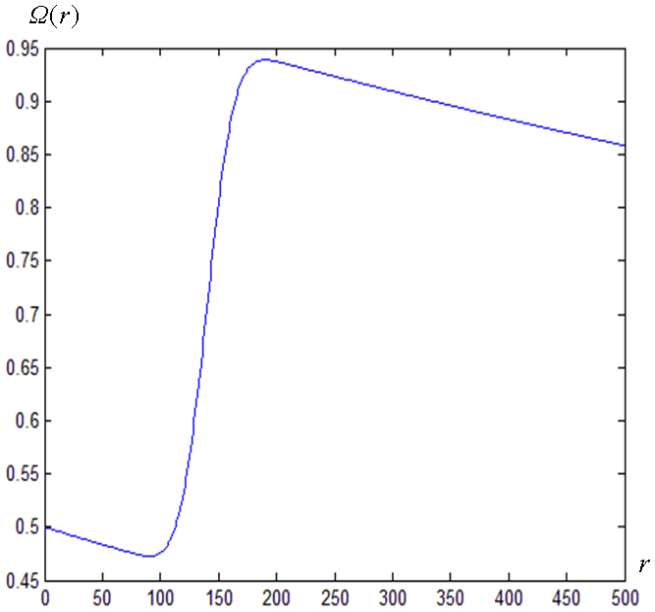

Рис. 3. Графическая зависимость функции (6).

Определение размера запаса элементов СрЗИ может быть выполнено *методом экспертной оценки* на основании данных, полученных при наблюдении за длительный период времени. В условиях необходимости содержания некоторого запаса для противодействия угрозам ИБ, связанным с несвоевременной доставкой элементов СрЗИ, ошибками в расчетах потребного количества, хищением и разрушением элементов, допустим, экспертно установлено значение $r = 400$.

Для оценки влияния размера запаса элементов СрЗИ на ИБ организации используем метод *шкалирования*, который применяется в условиях отсутствия статистических данных и сложности применения аналитических методов *присвоения числовых значений* отдельным атрибутам некоторой системы [18-21].

Не ограничивая общности, примем допущения:

- вероятность реализации угрозы ИБ Z_4 в сценарии (рис. 1) для $r = 171$ незначительна – $Q_4 = 0,01$ (при $Q_1 = Q_2 = Q_3 = Q_5 = 0,01$);
- при увеличении размера запаса на порядок $r = 1710$ вероятность реализации угрозы ИБ Z_4 оценим как $Q_4 = 1$;
- для задания взаимно однозначного соответствия между значениями Q_4 и r будем последовательно уменьшать рассматриваемый интервал, используя его крайние значения, по правилам:

(7) $$r_n = \frac{r_i + r_j}{2},\ Q_n = \frac{Q_i + Q_j}{2},$$

где r_n – усредненное целое значение r на рассматриваемом интервале; r_i и r_j – крайние целые значения r на рассматриваемом интервале; Q_n – усредненная оценка вероятности реализации угрозы ИБ Z_4; Q_i и Q_j – оценки вероятности реализации угрозы ИБ Z_4 при значениях r_i и r_j на рассматриваемом интервале.

Фрагмент шкалы соответствия, полученной с использованием правил (7), представлен в таблице 1.

Таблица 1. Фрагмент шкалы соответствия между r и Q_4.

r	оценка вероятности Q_4
171	0,01
400	0,15
⋮	⋮
1710	1

Для $r = 400$, согласно таблице 1, $Q_4 = 0{,}15$. Тогда с учетом $Q_1 = Q_2 = Q_3 = Q_5 = 0{,}01$ на основании (4) $k = 0{,}005$. Приведем в единой системе координат графические зависимости (6) для значений $k = 0{,}001$ и $k = 0{,}005$ (рис. 4). Из рис. 4 видно, что (6) принимает максимальное значение при запасе $r_R = 190$. Вероятность обеспечения элементами СрЗИ при $r = 400$ будет меньше в силу большего влияния издержек, связанных с хранением излишествующего запаса элементов.

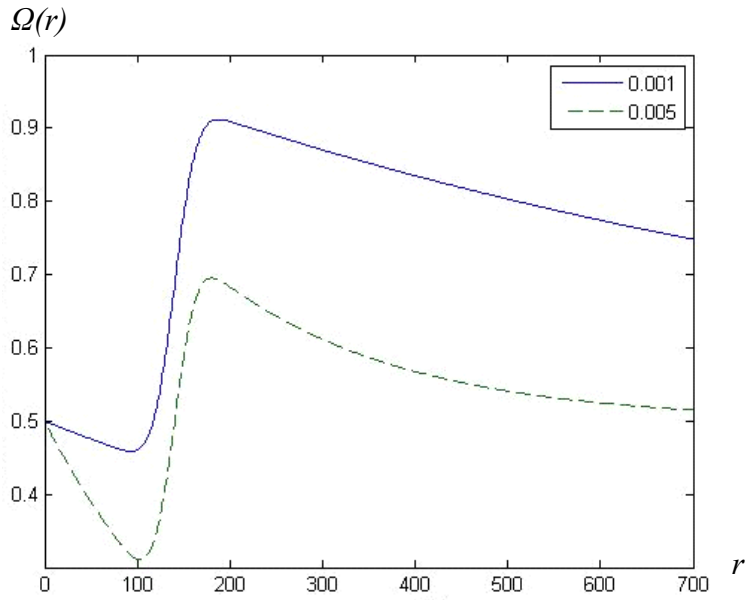

Рис. 4. Графические зависимости (6) при $k = 0{,}001$ и $k = 0{,}005$.

3. Заключение

Опыт решения многих задач исследования операций и управления запасами свидетельствует о том, что целевая функция в окрестности оптимума меняется медленно [22, 23]. В сочетании с неизбежной погрешностью исходных данных это оправдывает приближенный расчет оптимальных размеров запаса элементов СрЗИ и различные допущения, которые приходится делать для получения решения.

Использование предложенных элементов методики оценки возможно в рамках математического обеспечения функционирования логистической информационной системы в условиях неопределенности и противодействия угрозам ИБ объекту информатизации и системе ЗИ.

Список литературы

1. ГОСТ Р 51275-2006 Объект информатизации. Факторы воздействующие на информацию. Общие положения. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст. М.: Стандартинформ, 2007. 11 с.
2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст. М.: Стандартинформ, 2009. 25 с.
3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст. М.: Стандартинформ, 2008. 8 с.
4. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст. М.: Стандартинформ, 2008. 31 с.
5. ГОСТ Р ИСО 9000-2008. Системы менеджмента качества. Основные положения и словарь. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 470-ст. М.: Стандартинформ, 2009. 35 с.
6. Яковлев А.В. и др. Криптографическая защита информации: учебное пособие. Тамбов: Тамб. гос. техн. ун-т, 2006. 140 с.
7. Таунсенд К., Фохт Д. Проектирование и программная реализация экспертных систем на персональных ЭВМ. Пер. с англ. М.: Финансы и статистика, 1990. 320 с.
8. Джарратано Дж., Райли Г. Экспертные системы: принципы разработки и программирование. М.: Вильямс, 2002. 1152 с.
9. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Дата введения 2011-12-01. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст. М.: Стандартинформ, 2011. 47 с.
10. Соколовский Е.П. Математическое обеспечение экспертной системы расчета потребности ключей для криптографических систем // Сборник научных трудов шестой международной научно-технической конференции INFOCOM 6. Ставрополь, 21-27 апреля 2014: Сборник научных трудов. Часть II. С. 485-489.
11. Соколовский Е.П., Финько О.А. Управление запасами средств защиты информации в условиях неопределенности // XII Всероссийское совещание по проблемам управления ВСПУ-2014. Москва, 16-19 июня 2014 г.: Труды. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2014. С. 9217-9226.
12. Вентцель Е.С. Теория вероятностей. М.: 1969. 576 с.
13. Бенинг В.Е., Королев В.Ю. Математические основы теории риска. М.: Физматлит, 2011. 620 с.
14. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ. М.: Высшая школа, 1989. 361 с.
15. Соложенцев Е.Д. Сценарное логико-вероятностное управление риском в бизнесе и технике. СПб.: Бизнес-пресса, 2004. 432 с.
16. Вишняков Я.Д., Радаев Н.Н. Общая теория рисков. М.: Академия, 2008. 368 с.
17. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2000. 248 с.
18. Шрайбер Д. Проблемы шкалирования. Процесс социального исследования. М.: 1975. С. 149-209.
19. Стивене С.С. Математика, измерение и психофизика. Экспериментальная психология. Т. 1. М.: 1960. С. 19-89.
20. Leinfellner W. Einfuhrang in die Erkenntnis- und Wissenschafts-theorie. Mannheim, 1965.
21. Guthjahr W. Die Messung psychischer Eigenschaften. Berlin, 1971.
22. Сакович В.А. Модели управления запасами / Под ред. М.И. Балашевича. Мн.: Наука и техника, 1986. 319 с.
23. Рыжиков Ю.И. Теория очередей и управление запасами. СПб.: Питер, 2001. 384 с.